Systematic Design for Privacy in Ubicomp

L Jean Camp
ljean@ljean.com
812 856 1865

Kalpana Shankar
shankark@indiana.edu
812 856
Indiana University
Bloomington, IN 47401

Kay Connelly
connelly@cs.indiana.edu

Abstract

In designing ubicomp systems the common practice is to select a framing of privacy from the range of definitions, and to use that to inform design. Yet this framing may not be the choice made by those who will interact with the design. We propose utilizing the design for values approach in order to leverage the complexity of privacy to improve designs. In design for values, also called value-sensitive design, every party that interacts with a system participates in developing a values statement. Design for values conceives of participants in ubicomp as stakeholders rather than as users and designers, while acknowledging that the interaction between different parties is limited by domain-specific knowledge. To support value-sensitive design in ubicomp and enhance the construction of a values statement, the paper presents an abbreviated overview of the various legal and philosophical constructs of privacy.

In summary, this paper discusses privacy in ubicomp as a design, social, technical, and policy issue; outlines research challenges presented by the technical and social dimensions of using sensor networks as a monitoring technology; offers a survey of the possible definitions of privacy; and justifies the need for a methodology for designing for privacy in ubicomp.

Keywords: K.4.1.f Computer milieu: computers and society: public policy issues: privacy
J.9.d Computer Applications: mobile applications: pervasive computing

1. Introduction

Ubiquitous and pervasive computing, also known as ubicomp, will result in large-scale transformational change as our environment becomes aware, active and responsive. Through the distribution of sensors and tags such as RFID, ubicomp environments become active as sensor data is processed, examined, then triggers response in the environment, particularly when that environment is the home. As a result, pervasive computing will be uniquely intimate in its interaction with those frequently called "users". Because of the intensity and consistency of this interaction it is most important that the understanding of privacy embedded in a ubicomp design corresponds to the understanding of the individual who must interact with the system on a continuous, intimate basis.

We describe the important differences in the perspective of privacy for the stakeholders (vulnerable residents of home, designers, caregivers, investors, etc.). We argue that the very complexity of privacy can be leveraged to serve all stakeholders. In contrast, we illustrate that diminishing the complexity of privacy inevitably diminishes the design itself. Value-sensitive design enables informed design by leveraging the diverse definitions of privacy rather than avoiding or simplifying them.

In this paper, we introduce the domain of interest, home health care, in Section 2. We discuss the theoretical and methodological framework for value-sensitive design in Section 3. In Section 4, we provide a comprehensive if brief overview of privacy perspectives. We close by arguing that the design for values framework offers unique promise for privacy in healthcare.

2. Home Health Care

Ubiquitous computing, commonly referred to as ubicomp, will result in a large-scale transformational change as our environment becomes aware, active and responsive. The intensity of this transformation requires an awareness of privacy. Ubicomp has the immense potential to improve our lives by improving our communication abilities: display activity levels of a remote relative [Mynatt, Rowan, et al. 2001] [Connely & Seik, 2005], automating common tasks (e.g. re-order medicines when they expire), assisting those with disabilities to participate more fully in society (e.g. text-to-speech for the visually impaired) and helping keep vulnerable populations safe (e.g. sending an alarm to a physician when a patient does not take critical medicines [Floerkemeier, & Siegemund, 2003]) Ubicomp also has the potential to lead us into an Orwellian society where every action of every person is monitored and recorded.

Designing for values in the context of informal care networks implies that the designer be sensitive to the cognitive abilities of the subject as well as needs of the caregiver. For example, there are early warning signs of dementia. A ubicomp system can leverage technology to help identify these signs, and provide tailored support for the care network depending on the progress of the decline. Monitoring data of different types and granularity should be collected at the different stages (i.e., as an elder declines or an injured person recovers) in order to maximize the efficacy of the system in helping the caregivers while remaining sensitive to the privacy of the care recipient. Thus, all data do not need to be collected all of the time, but rather targeted data can be compiled and analyzed based on a risk profile.

Privacy need not mean less information, but rather more thoughtful use of data. Indeed, monitoring data of different types and granularity should be collected at the different stages (i.e., as an elder declines or an injured person recovers) in order to maximize the efficacy of the system in helping the caregivers orthogonal to the issue of remaining sensitive to the privacy of the care recipient.

There are a variety of off-the-shelf sensors available for use in the home. Different sensors in different contexts may require different types of filtering in order to maintain privacy and provide adequate information. Filtering can be implemented by reducing sample rates, reducing data precision, or aggregating data. For example data may be collected at fewer times, reported in time ranges rather than time-stamped, or reported only as an aggregate.

Current home-sensor systems collect as much information as possible by default. Data filtering is typically performed at the applications layer, with data storage being a distinct question. One way for designers to address privacy is to select appropriate filtering that can be done before data are stored, thereby protecting detailed information by never compiling it.

Decreased data availability also means less data to be lost in case of loss of machine security. Individuals left to manage their own home system are unlikely to be effective security managers. When interviewed people may present themselves as effective security managers, but available data indicates that their practices are woeful. Users' practices are little more than token behaviors

designed to prevent some unknowable harm that is not understood. The behaviors described in the ethnographic paper are best understood not as security behaviors but as flawed judgments under uncertainty. (Dourish, Grinter, Delgado de la Flor & Joseeph 2004)

Physical security is understood by the users. Network security is not, and thus their decisions are based on far more uncertainty. For example, Dourish offers an example of holistic security where the user secures her physical space to protect confidential information. How does the location of the screen alter in any way a network attack, Trojan horse, or viral infection? Not at all. The user is applying a completely inappropriate physical heuristic to network security.

Checking self-asserted domains is a common mechanisms for security. This cannot ensure documents are not infectious unless malicious parties are honest about their origins. Spam, phishing, 419 fraud, and viral attacks indicate that this is misplaced trust. (Dourish, Grinter, Delgado de la Flor & Joseeph 2004)

Practices users describe as practical management are often bad user heuristics that systematically fail to mitigate network security threats and often exacerbate them. The response of those with security training is to understand that ignorance is dangerous and hope to mitigate this through training. Yet educating users to the technologists' level of understanding is not feasible. Translation of stakeholder models of data protection to effective action requires matching stakeholder concepts of data control to that of the designer in order to provide useful and meaningful practices, as opposed to targeting and changing end users. The heuristics selected by the user to manage their own systems reflect not a rational evaluation of risk, but do reflect their own perceptions of the importance and nature of security. Therefore matching user perception to design goals can create a more understandable, and thus manageable, system.

The designers of security systems have failed to communicate requirements to users, so the only effective user behavior identified in the study is depending upon others. With in-home ubicomp, there is no information technology services staff. The only effective mechanisms users present upon investigation is either completely unavailable for in-home ubicomp, requires a concentration of trust that lends itself to the dystopian. End users cannot be effective security or privacy managers without a match between design, perception, and resulting heuristics.

3. Value-Sensitive Design

Value-sensitive design is a design method whereby the initial design is accompanied by a values statement. The values statement is explicitly not a Software Development Impact Statement because, while values choices can be made in design, value choices can also emerge during use. Design for values as a method embeds explicit values choices, documents those choices, and thus enables adoption and alteration of technologies to be informed choices made in the appropriate social context. Design with values as a critical component has been used successfully for location-based computing but not in home health care. (Freier, Consolvo, Kahn, Smith & Friedman, 2005).

In the case of ubicomp a values statement can be developed by the party to be monitored, the care-giver who will interact with the monitored party, the party paying for development, and the technologists. Values statements can be more straight forward in home-based systems as the stakeholders can be more easily identified. Contrast the situation to that of a university, where there are often literally thousands of stakeholders. [Camp, 2003][Friedman, 2001]

The sheer complexity of understanding a value as amorphous as security, which is itself better specified than privacy, has been a serious difficulty in applying value-sensitive design. [Nissenbaum &

Felton, 2002] Thus rather than developing a single monolithic concept of privacy, designers may build upon the previously extant definitions to create a common understanding between themselves and stakeholders. Without stakeholder definitions of privacy, designer concepts of privacy cannot protect those issues critical to the stakeholder.

Age, gender, education and earnings all influence individual perceptions of digital privacy. A ubicomp designer developing an installation for an elderly person is likely to differ from that stakeholder *in every significant dimensions*. There is no theoretical basis for assuming that the designer and stakeholder will have the same conceptions of privacy. For example, an elder may fear falling in the bathroom while a designer may still be dealing with his or her sexual identity. Thus an elder may seek real-time audio connection without limited data compilation over the long term, while a young person may be concerned with audio, especially audio that becomes active at some noise threshold. As a result, the elder may want different sensor monitors where the designer would tend to a zone of privacy due to the designers' discomfort rather than the stakeholders' requirements. In contrast, the elder may be sensitive to others' knowledge of the sheer number of visits to the bathroom, something that would not concern most youthful designers but would easily be evident with long term data compilation.

Design for values is not exclusively technologically deterministic, recognizing that the initial design may be altered during use. Thus design for values requires stakeholder participation in construction a values statement to guide the design not a specification of final design outcomes. The technologically deterministic [Eisenstein, 1979] [McLuhan, 1997], socially constructed [Fischer, 1994] [Spar, 2002] and dynamic iterative [Castells, 1997] [Douglas, 97] models of technological development have clear parallels in, respectively, the technical, preexisting, and emergent models proposed for computing systems in design for values [Friedman & Nissenbaum, 1996]. Technical bias is that which is inherent in or determined by the technology. Preexisting bias is that bias which had been previously socially constructed and is integrated into the technology. Emergent bias develops as a system is used and develops in a specific social context. The goal in value-sensitive design is not to create omniscient designers, but rather ethical design (within the designers' informational space) that enhances social discourse about any specific technological artifact. The participation of stakeholders may allow them to be informed and observant as they adopt the technology in their own social contexts.

Clarification of values is particularly important in discussing security and privacy, as these are so often confused in both technical design and user perception. While computer security and privacy are, in most cases, well aligned, they are not equivalent. Security is the control of information. Privacy is the control of information by the subject of the information. With personally identifiable information, the inability of the subject to control information linked with his/her identities is a threat to privacy.

While there is no known predictable method for making an absolute assertion about the privacy implications of a given default in a particular feature for a generic system, clearly predictions can be made about the potential for privacy violations created in a particular technology [Camp, 2001] [Lessig, 1999]. Although much research on privacy is applicable to ubiquitous computing and there are nearly 150 privacy enhancing technologies on the market, as well as dozens of innovations submitted every year to the Privacy Enhancing Technologies workshop, there has been inadequate examination of the potential application of these technologies in the context of home-based ubicomp for care-giving, potentially one of the most extreme cases in terms of privacy.

4. Theoretical Foundation: Privacy as a Design Value

On the surface, there is a seemingly inherent tradeoff between ubicomp and privacy. Privacy-enhancing ubicomp is not an oxymoron. Privacy and ubiquitous computing can, together, serve to

enhance individual autonomy. Of course, there is an conflict between the designer's desire to have information to make optimal use of the system and the subjects right to privacy, that is, their control of information about themselves. Yet carefully selecting information and deciding in the design stage who will have access to and control of information can enhance functionality while protecting privacy.

Making privacy function in ubicomp requires understanding the various dimensions of privacy. The technology implemented by a designer can vary based on the designers' conception of privacy (e.g., Phillips, 2004; Camp & Osorio, 2003). Thus in the following section I examine different conceptions of privacy, for Constitutional law to technical practice.

Complex definitions of user-centered privacy incorporate computer security, an understanding of the theoretical foundation of legal rights, and an appreciation of data protection. In this section the most common ubicomp approach (privacy as the creation of boundaries) is augmented by addition conceptions of privacy drawn from the legal and technology studies literature. None of these are original; all are widely used within the legal or science studies domains.

Privacy as Spatial

Privacy in ubiquitous computing is most often conceived of as an issue of boundaries. [Jaing, 2002] [Langheinrich, 2002] [Boyle, 2003] [Geraci, 2004] Many ubicomp designers have adopted a concept of contested social spaces as articulated in the concept of privacy as process. [Altman, 1975] These conceptions are important, informative, but inadequate.

The boundary concept strongly parallels the early work on regulation of speech on the Internet, in which legal and policy scholars disputed the nature of cyberspaces.[1] [Naughton, 1992] [Sunstein, 1995] In both digital speech and ubicomp privacy, spatial metaphors were adopted because of the potential power of the heuristic. Spatial metaphors enabled the classification of contests with historical conflicts of speech. Spatial metaphors offer great subtlety. Like the speech debate, the spatial ubicomp privacy discourse has integrated issues of social, natural and temporal spaces. [Langheinrich, 2002] Again mirroring the speech debate, ubicomp researchers are finding that while spatial metaphors offer insight, they offer little practical design guidance. In the case of speech, the DMCA clarified the issue of liability and requirements for oversight. Unlike in the case of speech, a legislative blow of Alexandrian strength cutting this Gordian Knot will not be soon forthcoming. Thus the following paragraphs build upon discourse from the speech debate to inform the subtleties of ubicomp design.

The difference between virtual and physical spaces is determined by the nature of the boundaries that divide them. Virtual boundaries are distinct in three dimensions: simultaneity, permeability and exclusivity. [Camp & Chien, 2001] Simultaneity refers to the ability of a person to be two places at once: at work and at a train ticket booth. Permeability is the capacity of ICTs to make spatial, organizational or functional barriers more powerful, less powerful, or even invisible. The permeability of the work/home barrier is most clearly illustrated with telecommuting. Barriers can be so permeable as to be transversed without the knowledge of the person putatively moving across the boundary. For example, moving from a conference site to the payment processor or from a web site to an affiliate is intended to be seamless. Similarly some blogs (a notably annoying feature

[1] This debate was settled when Internet Service Providers obtained a Safe Harbor provision in the Digital Millennium Copyright Act that delineated appropriate ISP behavior with regards to copyright (a most troublesome modern speech/property conflict) and expression.

dropped by e-commerce sites) keep a reader framed so that the reader cannot easily escape one blog into another. In one case the user crosses boundaries and experiences simultaneity, and in the other the user attempts to cross boundaries and is constrained by invisible ties.

Exclusivity, in contrast, is the ability of ICTs to create spaces that are impermeable, or even imperceptible, to others. Intranets may offer exclusive access through a variety of access control mechanisms, and the creation of databases that are invisible to the subjects clearly illustrates the capacity for exclusivity. In the physical sphere, the walled private developments offer an excellent example of exclusivity, yet it is not possible to make physical spaces so exclusive as to be invisible. In digital spaces discovery of places one is not allowed to view is itself problematic. Technologies redefine the nature of space, and digital networked technologies alter the nature of boundaries. [Shapiro, 1998]

The ubicomp community currently embraces a spatial metaphor for privacy. Spatial metaphors have proven too blunt for privacy and speech on the Internet, and are likely to prove inadequate for ubicomp. Spatial metaphors are an important but inadequate start; a foundation but not a endpoint.

Data Protection

Due to the complexity of the problem of privacy and ever increasing data flows, the European Union, Canada, and Australia have adopted data protection regimes. The Code of Fair Information Practice is the foundation of the dominant data protection regimes. The Code (and the related data protection requirements) has as its core *transparency, consent, and correction*. In terms of privacy, these are generally seen as a reasonable minimum. However, in the case of designing for home-based medical ubicomp, even the Code, which is far more simple that the European or Canadian data protection regimes, is problematic.

Transparency requires that no data compilation be secret. Of course, that is implicit in the installation of a sensor network in one's home. Yet consent can be problematic even when the installation is clearly visible. Informed consent implies an understanding of the underlying sensor technology and the data that can be compiled. "This is a pressure sensor", may not convey adequate information if the pressure sensors and software are such that they can uniquely identify those walking across the space. Consent includes not only awareness of the existence of data in sorted form, but also consent to the various uses of that data. Consent requires that data can be deleted or corrected when desired by the subject.

The capacity to alter data, included in the requirement that individuals are allowed to ensure data are correct, obviously has distinct implications when the data are stored locally and the individual may not perceive correct data as being in his or her own interest. For example, elders with dementia may delete necessary data.

A more general call for use of data protection principles in ubicomp originated in 2001 [Langheinrich, 2001] yet the spatial model remains dominant. Data protection principles above have been dissected for appropriate application in ubicomp. [Jiang, Hong, Landay, 2002] The core principles of data protection were inadequate for general application. The tasks required by data protection - collection, access, and secondary use limitation – were respecified for the ubicomp environment. Data subjects in any case must be empowered by being able to limit data collection, choosing to avoid date surveillance, and be aware of all data compilations. These correspond to the fair information practices above, but the ubicomp environment required an extension to data

protection into a user-centric and technology-centric parsing to simplify application of the concepts to specific designs.

Data protection defines some data as inalienable (e.g., sexual orientation) and other data as subject to contract (e.g., name, address, date and amount of a purchase) Yet these constraints may not be adequate in ubicomp. The clean, carefully drawn lines about particular data elements in data protection are inadequate for the continuous data flow with probabilistic potential to detail all factors of our lives.

Autonomy

Data protection regimes have the advantage of mitigating the complex dimensions of privacy. In contrast, spatial and multi-level jurisdictional approaches have the advantage of illuminating the sometimes competing dimensions of privacy. This and the following two sections describe the jurisdictional approach.

Autonomy has traditionally been a central concern of legal scholars in privacy. In the literature of democracy, privacy is autonomy. Privacy as a Human Right under the UN Universal Declaration of Human Rights is based on the freedom to act without the fear of surveillance. Surveillance can result in targeted retaliation. Similarly, the European Data protection regime recognizes informational autonomy by declaring that there are data that *cannot be collected* except under highly constrained circumstances, for example data on sexual preference. Legal monographs on privacy tend often focus exclusively on the autonomy concept of privacy (e.g., Alderman and Kennedy, 1995).

(Notice that the use of word and concept of autonomy in privacy does not directly map to autonomy as broadly conceived in health care. At the grossest level, the consent-based concept of autonomy in health care is more closely aligned with the data protection model in privacy. More detailed discussion of autonomy as perceived by health professionals and in health practice is beyond the scope of this work. Suffice to say that the same word refers to two different and significant bodies of literature and practice, and this focus is on the non-medical legal tradition.)

Privacy is a form of autonomy because a person under surveillance is not free. In the United States, Constitutional definitions of privacy are based on autonomy, not seclusion. These decisions have instituted both sexual autonomy and, in the case of postal mail and library records, a tradition of information autonomy under the law. (This concept of information autonomy was altered under the USA PATRIOT Act but still remains central in American jurisprudence.)

Autonomy is more than agency. Autonomy is the ability to act without threat of retaliation and thus refers to freedom of action that is not mitigated by surveillance. In NAACP v. Alabama, the opinion sums up the requirement for autonomy for a legal regime, "a government purpose to control or prevent activities constitutionally subject to regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms." A technical modification may be "a technological purpose to control or prevent activities subject to surveillance may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of preferred freedoms."

Autonomy as privacy became part of the popular discourse in the United States in 1965 because of two decisions by the Supreme Court that year. In the first, a unanimous Court struck down the Congressional statutory authorization of the Post Office to detain mail the USPS

determined to be "communist political propaganda" and to release that mail only after the addressee notified the USPS in writing that he or she wanted that specific information. (Lamont v. Postmaster General) Later the Court reviewed an arrest of a Director of Planned Parenthood who was providing contraception and information about contraception to a married couple. The law prohibiting such communication was abolished in a split court with the decision Griswold v. Connecticut. These two decisions form the underpinning of the right to privacy. Both are decisions based on the *availability of information.*

In a world of ubiquitous computing, individual access to information judged dangerous, harmful or simply protected by the government will be widely available given common data marketing practices. Common daily routines can illustrate such basic choices as religious and sexual practices. Once compiled, such information will be difficult to secure, given common coding practices. Under the autonomy understanding of privacy, consent to compile such data is not adequate to mitigate privacy concerns. A person cannot consent to give up core freedoms. (Notice this is in opposition to the concept of autonomy and its relationship to informed consent in health care.)

Privacy as autonomy, privacy as a human right, is inalienable. Only the concept of privacy as autonomy provides the theoretical underpinning for individuals' interest in data about themselves absent quantified harm. Recognizing that individuals have interests in data that extends beyond immediate harm is a recognition of the right to privacy as autonomy.

In technical systems, privacy as autonomy is usually implemented as strong anonymity. Users who seek autonomy in a particular dimension will seek data deletion, anonymity or obfuscation. The Cricket system implemented an autonomy model of user interaction where users could be anonymous and still access data. The Cricket designers did not use an explicit value-sensitive design approach, but did explicitly design to value privacy. As privacy as autonomy is the strongest privacy model, providing autonomy by design can address all stakeholder privacy concerns.

Property

Privacy in the United States is a subject of both civil (i.e., state law) as well as federal Constitutional law. Thus privacy is also a tort (or rather a set for four torts that need not be specified here) in the United States. Privacy as a tort defines privacy as essentially commercial, a wrong that can be set right by payment.

Privacy can yield economic advantage to select stakeholders. [Bloustein, 1968] [Mell, 1996] For example, ubicomp that provides demographic information and thus enables price discrimination can violate this dimension of privacy. Ubicomp that identifies intensity of medical need could dramatically alter pricing by making health insurance unaffordable, as the US has a market-based medical financing system.

User behavior with respect to personal information, valuation of protection of information, and characterization of data types with respect to the subject identification are all topics of active economics research. [Camp & Lewis, 2004]

The objection to privacy as property is that property rights are alienable. Under the property paradigm all subject interests in property are lost at the transaction. A data subject has no more right to limit secondary use of data than a seller of a home has a right to return and paint the kitchen after the closing. [Samuelson, 2000]

In either case, the data are economically valuable and thus centralized authorities will have economic incentives to share those data. [Odlyzko, 2004] Users who see data as property will want payment for data. Alternatively, users may seek deniable pseudonyms in order to avoid future price discrimination.

Privacy Concepts as Complementary

The wealth of articulated viewpoints on privacy can serve to inform design. Recognizing that these models of privacy exist is not to dictate design specifics. Autonomy is too subtle to be addressed via a single computational mechanism and requires interaction between designer and stakeholders, to ensure technology enhances and does not constrain activity. Autonomy can also identify activities that can offer spatial guidance, for example avoiding sensors in areas in the home designed for sexual activities or prayer. Privacy as the right to seclusion complements the boundaries model. Privacy as property provides a market mechanism or transactional model to enable conflict resolution in the boundaries model. Alternatively, privacy as property can ensure payment of subjects. Privacy as data protection offers a well-developed framework, including implementing legislation in more than a dozen nations, that create a set of well-defined questions. Each of these perspectives can assist in informing designers about privacy implications and assist participants in articulating privacy concerns.

As an example, one idea that invites critique is to put a sensor on a bed to obtain weight information, to collect information real time, and to provide the information to those interested in a vulnerable person's weight. In this case the boundary definition could assist in improving the design – is there no less private place than a bed one can place a weight sensor? The data protection perspective would help – is there any conceivable need for constant real time data? And the understanding of privacy autonomy would be enlightening – would activities in the bed be altered by the existence of the surveillance? (Dourish, 2004)

One design not created to invite critique but to enhance privacy instead does the former: the system by Hengartner & Steenkiste. [Hengartner & Steenkiste, 2004] This system is fatally flawed from consideration of privacy as strictly spatial. The core assumption is that space is hierarchal and thus location determines individual privacy rights without regard to the nature of the individual. Thus, in the design the location governs the availability of data of the subject, over the rules set by the subject. For example, a student who has obtained an order of protection from another student may be tracked by the threatening student via this system. (Such orders are regularly issued by the university.) The threatening student could obtain location information in public places (e.g., a classroom). The system alters the risk profile by making the personal information anonymously, immediately, and remotely available. This system is flawed because of its absolute dependance on physical spatial concepts mapping perfectly to virtual spatial concepts and its failure to consider any alternative. No data are filtered other than that specified by location owners. By implementing a narrow concept of centralized access control as security, this system has increased exposure of personally identifiable information, prohibited personal control of data, and decreased individual autonomy.

Privacy by design, as in the Cricket system, enables both location services and individual privacy [Priyantha & Chakraborty, 2000]. In this case, the location offers relevant information that can be requested by users. The only authorization required is physical location. Therefore, by using verifiable assertion of location, the location service can determine the authorization required for data access, and the default is anonymity of the requestor. In this case the data are public (e.g., relative location, available nearby services such as printers or food) The individual is able to access information based on the relevant information (i.e., location) without losing privacy. The system enables autonomy through

anonymity of service requesters and integrates data protection through minimal data provision, and data control by requesters.

Another case where privacy was brought into the design is Intel's CareNet project, which performed extensive user studies which included examining the issues surrounding privacy with home-based ubicomp [Consolvo, Roessler, & Shelton, 2004]. In this case, caregivers and those who were subject to monitoring defined the monitored activities. The designers translated the non-technical explanations of activities (e.g., makes coffee by 8am) into system design. The monitoring was carefully targeted so all generated data would be of interest. This method was very close to value-sensitive design described here.

5. Closing

The implications of ubicomp have the potential to be of particular importance in an area experiencing rapid change: home-based health care. The amount of informal care given to elders is likely to increase as the baby-boom generation starts to use, and threatens to overload, currently available assisted-living and nursing home facilities. Indeed, the number of people over the age of 65 in the US is projected to double in the year 2030 to almost 69 ½ million. This is an increase from 8% to 22% of the entire US population [US Agency on Aging, 1998].

Failing to embed privacy in the design on the basis of the demographics for home-based ubicomp risks instantiating a standard of surveillance for all ubicomp. There is a very real possibility that the designs for the vulnerable and elderly population will set the standards for home-based ubicomp design. Instantiating design standards that dismiss privacy for the vulnerable will reduce privacy for all. As such, it is essential that research in this area address the issues of privacy surrounding sensing and monitoring technologies in the home.

Current technological design methodologies, such as computer supported cooperative work and user centered design, may prove too resource intensive for the design of systems specific for individuals. Privacy can and must be made off-the-shelf and customizable as ubicomp becomes off-the-shelf and customizable. Value-sensitive design combines a focus on the technological artifact (e.g., the sensor) with an appreciation of the context. VSD provides a method for rejecting the false choice of ubicomp versus privacy, and embracing the autonomy promised by home-based ubicomp for vulnerable populations.

6. References

Alderman, E. and Kennedy, C., (1995) *The Right to Privacy*, Alfred A Knopf, New York, NY.

Altman, I. (1975) *The Environment and Social Behavior*. Irving Publishers, New York, NY.

Bloustein, E. (1968) "Privacy as an aspect of human dignity: an answer to Dean Prosser." *NY Univ. Law Review* 39: 962-970.

Boyle, M. (2003) "A shared vocabulary for privacy", *Privacy in Ubicomp*. Berkeley, CA.

Camp, L. J. (2001) *Trust and Risk in Electronic Commerce*. Cambridge, MA, The MIT Press.

Camp, L. J. (2003) "Design for trust". T*rust, Reputation, and Security: Theories and Practice*. R. Falcone. Springer/Kluwer, Berlin.

Camp, L. J. (2004) "Digital identity." *IEEE Technology & Society* 23(3): 34-41.

Camp, L Jean & Y.T. Chien, "The Internet as Public Space: Concepts, Issues and Implications in Public Policy," *Readings in Cyberethics*, eds. R. Spinello and H. Tavani, Jones and Bartlett Publishers (Sudbury, MA) 2001. pp.111-123.

Camp, L. J. & S. Lewis (2004) *Economics of Security*, Springer, Berlin.

Camp, L. J. & C. Osorio (2003) "Privacy Enhancing Technologies for Internet Commerce" *Trust in the Network Economy*, Springer-Verlag, Berlin.

Castells, M. (1997) *The Information Age: Economy, Society, Culture*. Oxford Univ., Blackwell Publishers.

Connelly, K., K. A. Siek, et al. (2005) "Designing a PDA Interface for Dialysis Patients to Monitor Diet in their Everyday Life", *HCI Int.'l 2005*, Las Vegas, NV.

Consolvo, S, Roessler, P. & B.E. Shelton, (2004) "The CareNet Display", *Proc. the 6th Int'l Conf. on Ubiquitous Computing: UbiComp '04*, (Sep 2004), pp. 1-17.

Douglas, S. (1997) *Inventing American Broadcasting 1899-1922*. The Johns Hopkins Univ. Press, Baltimore, MD.

Dourish, P. , Grinter R., Delgado de la Flor, J. and Joseeph M. (2004) Security in the Wild, *Personal and Ubiquitous Computing*, Vol 8, No 6, pp 391-401.

Eisenstein, E. (1979) *The Printing Press as an Agent of Change*. Cambridge Univ. Press, Cambridge, UK.

Fischer, C. S. (1994) *America Calling: A Social History of the Telephone to 1940*. Univ. of California Press, Berkeley, CA.

Floerkemeier, C. and F. Siegemund (2003) "Improving the effectiveness of medical treatment with pervasive computing technologies", *Ubicomp 2003*, Seattle, WA.

Freier, N. G., Consolvo, S., Kahn, P. H., Jr., Smith, I., & Friedman, B. (2005). "A Value Sensitive Design Investigation of Privacy for Location-Enhanced Computing". *Quality, Value(s), and Choice: Exploring Wider Implications of HCI Practice,* CHI2005. Portland, OR. www.ischool.washington.edu/vsd/files/freier05values_workshop.pdf

Friedman, B., Ed. (2001) *Human Values and the Design of Computer Technology*. Univ. of Chicago Press, Chicago IL.

Friedman, B. and H. Nissenbaum (1996) "Bias in computer systems." *ACM Transactions on Information Systems (TOIS)* 14(3): 330-347.

Geraci, J. (2004) "Community and Boundary in the Age of Mobile Computing: Ubicomp in the Urban Frontier". *Privacy in Ubicomp*. Nottingham, UK.

Hengartner, U. and P. Steenkiste (2004) "Implementing Access Control to People Location Information". *9th Symp. on Access Control Models and Technologies* (SACMAT 2004), Yorktown Heights, NY.

Jiang, Hong, Landay, (2002) "Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing", *Proc. the 4th Int.'l Conf. on Ubiquitous Computing Theory*, Goteborg, Sweden, Sept 29 – Oct 1.

Jiang, X. (2002) "Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces". *Privacy in Ubicomp 2002*.

Langheinrich, M. (2002) "Privacy Invasions in Ubiquitous Computing", *Privacy in Ubicomp 2002*. Goteborg, Sweden.

Langheinrich, M. (2001) Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. *Proc. Ubicomp 2001*. Atlanta, GA.

Lessig, L. (1999) *Code and other basic laws of cyberspace*. NY, Basic Books.

McLuhan, M. (1977) *The Gutenberg Galaxy*. Univ. of Toronto Press, Toronto, CA.

Mell, P. (1996) "Seeking shade in a land of perpetual sunlight: privacy as property in the electronic wilderness." *Berkeley Technology Law Journal* 11(1): 1-92.

Mynatt, E. D., J. Rowan, et al. (2001) "Digital family portraits: Providing peace of mind for extended family members". *Proc. the ACM Conf. on Ubicomp*, Vol. 81, 409-441.

Naughton, E. J. (1992), "Is cyberspace a public forum? Computer bulletin boards, free speech and state action," *Georgetown Law Journal*, Vol. 81, 409-441.

Nissenbaum, H., E. Felton, et al. (2002) "Computer security: Competing concepts", *30th Research Conf. on Comm., Information and Internet Policy*, Wash., DC.

Odlyzko, A. (2004) "Privacy, Economics, and Price Discrimination on the Internet in Economics of Information Security", *Economics of Information Security* eds. Camp & Lewis.

Phillips, D. J. (2004) "Privacy Policy and PETs: The Influence of Privacy Regimes on the Development and Social Implications of Privacy Enhancing Technologies", *New Media & Society,* Vol 6, No 6, pp 691-706.

Priyantha, N. B., A. Chakraborty, et al. (2000) "The Cricket Location-Support System", *Proc. 6th Mobicomp*, Boston, MA.

Samuelson, P., (2000) Privacy As Intellectual Property? *Stanford Law Review* V. 52, pp. 1125.

Shapiro, S. (1998) "Places and Space: The Historical Interaction of Technology, Home, and Privacy", *The Information Society*, 4(1): 275-284.

Sunstein, C. (1995) "The First Amendment in Cyberspace" *Yale Law Journal*, Vol 104, pp1757-1804

US Agency on Aging (1998) *Profile of Older Americans*. US Govt. Printing Office, Gaithersburg, MD.

US Government Accountability Office (1998) *Long-Term Care: Diverse, Growing Population Includes Americans of All Ages*. US Government Printing Office, Gaithersburg, MD.

Warren S. and Brandeis L., 1890, "The right to privacy," *Harvard Law Review*, Vol. 4, pp.193-220.